

Published and Copyright (c) 1999 - 2004
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Kevin Savetz

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

<http://people.delphiforums.com/dpj/a-one.htm>
<http://www.icwhen.com/aone/>
<http://almag.atari.org>
Now available:
<http://www.atarinews.org>

Visit the Atari Advantage Forum on Delphi!
<http://forums.delphiforums.com/atari/>

=~==~==

~ AOL Spam Levels Down! ~ U.S. Still Spam King! ~ AtarIRC Upgraded!
~ 2004 Security Ratings ~ HighWire Update Out! ~ China's New Web!
~ New Version of Hatari! ~ FreeMiNT/XaAES News! ~ Ausbruch for Falcon!

-* eBay To Drop Passport Support *-
-* Net Sales Tax May Be Reality in 2005 -
-* Microsoft Settlement Dollars Not Claimed! *-

=~==~==

->From the Editor's Keyboard "Saying it like it is!"
"~~~~~"

Happy New Year 2005 to you all!! It's been one helluva year; the new year has to be a better one (don't we say that every year!?).

It's hard to believe that we're starting our seventh year of publication. It seems like yesterday that Joe and I decided to start A-ONE. The time has certainly flown by. There have been a lot of memories prior to this mag, and they continue. While the Atari scene is no way near what it was when we both started writing for Atari-related magazines, it's still something that holds us together.

We'll keep this week's commentary short this week - pending celebrations, you know. Have a safe New Years!

Until next time...

=~==~==

HighWire 0.2.4 Released

Hi all,

Following a bunch of other software releases this Christmas holiday, we now bring you a new update to the web browser HighWire!

The 0.2.4 release offers some new options that has been requested for a while. One of them being the ability to define a start page of your own choice. Internally the program is now able to put dialogs into GEM windows, although so far only the SHIFT+CTRL+O is taking advantage of this addition.

Hades users should be pleased to learn that HighWire now supports high/true colour screenmodes (24/32 bits) for Hades graphic card drivers. This means that they will now finally be able to view images in correct colours! In addition to this, the palette parsing for XPMs has been improved in order to get more of such images decoded accurately.

One of the more serious bugs ironed out in this release was one that would

cause endless attempts of loading CSS files when such a file was empty or missing. Another outstanding issue that has been resolved recently was a problem with downloading images from HTTPS sources. Another thing that has changed is that HighWire will now avoid reloading a page from remote when base font setting is changed.

In the menu bar you can now find the new entries "View Images" and "Use CSS". When the option "Cookies allowed" is changed from the menu bar, the config file will be updated accordingly.

These are the most noticeable changes, please refer to change.log for additional details.

To download and read more, visit us at: <http://highwire.atari-users.net>

Thanks!

/HighWire development team

AtarIRC v2.00 Released

Main additions are:

- Tab like scheme for multiple scrollback buffers
- Separate log files for channels and queries
- Public IP and DCC port mapping to get around router problems
- other misc changes and bug fixes, see docs for details

<http://www.bright.net/~gfabasic/>

New Falcon Game: Ausbruch

Foundation Two proudly released a Falcon 030 game called:

Ausbruch

The game was in the game compo at the outline party this year. After the party some bugs was fixed, and now the game is ready.

<http://www.foundationtwo.de>

Hatari Version 0.60 Has Been Released

T. Huth has announced:

Version 0.60 of the Atari ST emulator Hatari has been released. It is mainly a bug-fix release, so there is not much new this time:

- Some code cleanup and bug fixes.

- The configuration file layout has changed a little bit (so you might have to check your settings in the GUI and to save the new configuration again).
- Window/fullscreen mode is now correctly initialized from the configuration file.
- Added --window command line option to force a start in window mode.
- Added alert boxes to show warnings, errors and information messages.
- PC mouse pointer is now better in sync with the ST mouse pointer.
- It's now possible to load an alternative cartridge image file.

<http://hatari.sourceforge.net>

FreeMiNT/XaAES Development Snapshot

GokMasE has announced:

A new development snapshot release of FreeMiNT/XaAES has been made available again, and this time you can expect a distribution mainly focusing on heavy bugfixing. While this version appears to be a nice leap forward when it comes to stability and accuracy, do keep in mind that it is alpha software!

That said, make sure to at the very least update both your kernel as well as the xaloader, mouse driver and XaAES kernel module!

<http://xaaes.atariforge.net/>

~~~~~

PEOPLE ARE TALKING  
compiled by Joe Mirando  
[joe@atarinews.org](mailto:joe@atarinews.org)

[Editor's note: Rumor has it that Joe is running around somewhere in Connecticut looking for that baby with the 2005-imprinted diaper. Little does Joe realize, that baby won't make an appearance until around midnight tonight!]

~~~~~

A-ONE's Headline News
The Latest in Computer Technology News

Online Sales Tax Enforcement May Become Certain In 2005

The proposed passage of federal legislation to enforce the collection of sales taxes on Internet sales is gaining momentum and is likely to become a major effort before Congress in 2005, as states and municipalities work to coordinate the effort to help fill their depleted treasuries.

The collection of online sales taxes, which has frustrated states for years, needs federal legislation to give the states the wherewithal to enforce the collection of the sales taxes. Most states currently require the collection of sales taxes on items bought over the Web and through catalogs, but most consumers don't know they are required to pay the taxes and most businesses don't charge for the taxes because they maintain the process is too complicated.

Senator Mike Emzi (R-Wyo.) has proposed legislation that would establish more uniform sales tax procedures throughout the nation and give individual states more power to enforce the collection of the sales taxes. Also aggressively promoting the legislation is Sen. Lamar Alexander, (R-Tenn.).

"Everything is at the critical state right now," said Jon Abolins of sales tax provider Taxware LP in an interview Thursday. "Eighteen states have enacted legislation and another 22 are working on it." Once the number of states hits a critical mass, the legislation's chances of final passage are enhanced, Abolins said.

"I think there's a better chance than even of getting the legislation this coming year," said Abolins. "There's no national election in 2005. State senators and lobbyists are all over Capital Hill pushing for the legislation."

As things stand now, sales taxes in most states " a few states have no sales taxes " are a patchwork quilt of regulations from state to state and from municipality to municipality. Much of the confusion centers on nexus " the situation in which a retailer has a store or other physical presence in a state. For instance, a retailer based in California would not have to pay sales taxes on items shipped to customers in New York if the retailer had no facilities or physical presence (nexus) in New York.

"The states are asking Congress to remove the nexus (issue)," said Abolins, who is senior vice president of operations at Taxware, which creates software that automates sales tax transactions. He noted that Congress does not want to levy any federal sales taxes, but simply wants to help states enforce their sales tax activities.

"Almost no states enforce sales tax collection," said Alolins, "It's up to the consumer to pay sales taxes, (but) most consumers don't know they should pay sales taxes voluntarily."

States have banded together to lobby for passage of the issue in the Streamlined Sales Tax Project. Another group that is lobbying to pass the federal legislation is the National Conference of State Legislations.

Microsoft Antitrust Settlement Dollars Going Largely Unclaimed

California companies and consumers who purchased Microsoft PC software may be leaving more than \$1 billion on the table as a deadline for filing in a California class action approaches.

The Settlement Recovery Center (SRC), which assists businesses and non-profits making claims in class actions, said less than one million claims out of a potential 14 million claims have been filed as of Monday in the California case. The deadline for filing is Jan. 8.

Attorneys in the class action led by San Francisco law firm Townsend & Townsend & Crew have been awarded \$101 million in fees and \$11.5 million in expenses. As things stand at the moment, the attorneys could make more money than the claimants in the class action.

"The California case is the first to expire," said SRC spokesman Craig Wolfson, noting that several states have won class action suits against Microsoft. "We have 600 or more clients in California representing over one million employees."

Many Californians and companies that purchased Microsoft software between 1995 and 2001 don't realize they can make claims in the class action, Wolfson said.

The California class action enables Microsoft users to obtain vouchers for Microsoft software in some cases, according to a complicated procedure for obtaining credit for Microsoft software and for purchased PCs with Microsoft software.

"It's a timing issue," said Wolfson, noting that there are different provisions for paying vouchers and monies according to different times when the Microsoft products were purchased. "And it's not just for software but it's also for computer gear."

"Companies don't understand what's at stake," said SRC founder and CEO Howard Yellen in a statement. "The Microsoft settlement is great, but it's not well understood. We have quite a few corporate clients who will recover over a million dollars each." Companies that upgraded Windows and Office software between 1995 and 2001 have the best chance of collecting, the SRC said, noting that 80 percent of the Microsoft settlement fees are scheduled to be awarded to companies.

Individuals don't have to provide documentation for much of their Microsoft purchases "they just need to fill out a simple form available on the Internet to claim up to five eligible purchases. For companies, the process is more complicated as they must file certain software licensing forms and other documentation.

EBay to Drop Support for Microsoft's Passport

Microsoft Corp. said on Thursday that eBay Inc. will soon drop support for its Passport service, originally intended to make the world's biggest software maker the gatekeeper of Web identities.

But Microsoft said it will keep Passport up and running, despite the loss

of one of its earliest and most important partners.

eBay said in a message to users on Wednesday that in late January it will stop allowing them to sign on to its Web marketplace through Passport.

Passport allows users to store such things as passwords and credit card information for use across the Web. With its launch in 1999, Microsoft aimed to insert itself in a key position in e-commerce transactions.

But the service has since fallen short of that goal due to several significant hurdles - including security and privacy concerns.

The move by eBay, far and away the most popular U.S. shopping Web site, ends a partnership forged in 2001 and underscores consumers' unwillingness to embrace Passport outside Microsoft's own MSN Internet network.

"A very small percentage of eBay users regularly signed in using Passport," said eBay spokesman Hani Durzy, who added that the company also has provided alternatives to users who receive eBay alerts through Microsoft's .Net service.

Passport swiftly met with resistance on several fronts.

The competitive response to Passport came in the form of the Liberty Alliance, a consortium of companies including Sun Microsystems Inc., Hewlett-Packard Co., American Express Co. and Sony Corp. The group's aim was to create standards for identifying people on the Web and to promote services to rival Passport.

Privacy groups and antitrust regulators weighed in with concerns, and in 2003 security experts unearthed a flaw that could have allowed scam artists to hijack older Passport accounts.

Retailers also balked at the prospect of having Microsoft at the center of online transactions and worried that it might one day try to take a cut.

Passport currently has 200 million users, many of whom use it to sign on to Microsoft's e-mail and instant messenger products. The company continues to be committed to providing authentication services to its partners, a Microsoft spokeswoman said.

AOL Spam Down 75 Pct; Net Spam Trends Reverse

You've got less spam, according to America Online, the world's largest online service.

The online unit of Time Warner Inc. on Monday said junk e-mail declined by more than 75 percent this year, based on its internal member reports.

Junk e-mail, known as spam, accounted for about 83 percent of computer traffic at one point this year, and have cost Internet providers about \$500 million in wasted bandwidth, analysts have said.

As of November 2004, AOL received an average of 2.2 million complaints daily from its more than 24 million subscribers, down from 11 million complaints in the same period last year.

The daily average number of e-mails blocked by AOL's spam filters fell 50 percent to about 1.2 billion e-mails in late 2004 from a peak of 2.4 billion in 2003.

Attempts made by junk e-mail senders also fell to about 1.6 billion daily, from 2.1 billion last year.

AOL launched a new version of its software, AOL 9.0 Security Edition in November, which included a free version of the McAfee VirusScan Online software and improved anti-spam tools.

The company is also part of an tech industry coalition comprised of Microsoft Corp., EarthLink Inc. and Yahoo Inc., which have vigorously gone after suspected e-mail marketers, who hide behind fake e-mail addresses.

Dutch Watchdog Levies First Fines Against Spammers

The Dutch telecom and postal watchdog OPTA has levied fines as high as 42,500 euros (\$57,540) against several individuals and small companies for sending out spam messages.

OPTA said in a statement on Tuesday the fines were for spam - a term widely used for unsolicited commercial e-mails, often hawking products to combat sexual dysfunction or promote weight loss - sent to both mobile phones and to e-mail addresses.

The fines were the first by OPTA against spammers. The body said they were levied in line with tougher European Union standards to combat a problem that is estimated to cost European businesses upwards of 2.5 billion euros a year.

The EU has tried to fight spam by introducing a ban on unsolicited e-mails in 2002, but the EU law is weakly enforced and several countries have not yet introduced it.

Anti-spam group the Spamhaus Project has listed Britain among its top 10 list of spamming countries.

U.S. Still Spam King

The U.S. has maintained its dubious distinction of being the world's top producer of spam, leading the "Dirty Dozen" list compiled by security authority Sophos by a wide margin.

After scanning all spam messages received at a global network of traps throughout the past year, Sophos researchers determined that the U.S. is responsible for exporting 42 percent of all mass e-mail attacks. South Korea is second, at 13 percent, followed by China (8 percent), Canada (6 percent) and Brazil (3 percent).

Despite such efforts as the CAN-SPAM act, which was passed in January, efforts to address the problem in the U.S. are having little impact, Gregg Mastoras, senior security analyst at Sophos, told NewsFactor. "The problem is poor legislation and a lack of interest among law enforcement agencies

to pursue spammers," he said, noting that the U.S. topped the previous "Dirty Dozen" list issued early this year.

Spammers are taking advantage of high-speed Internet connections, Mastoras noted, with South Korea, which has the greatest penetration of broadband technology of any country, maintaining its position as a leading producer of spam.

They are also getting better at using the skills of virus writers to create "zombie" computers that are directed to launch spam attacks without the users' knowledge. Mastoras said some 40 percent of the world's spam is distributed via such compromised machines.

As long as there is an opportunity to make some easy money with relatively little risk, spam producers will find a way to ply their trade, said Mastoras. He pointed out that Canada did a better job fighting spam this year than in 2003, primarily because the government established a task force to focus on the problem and made some high-profile arrests that served as warnings.

The Sophos list arrives at the same time Internet portal America Online reports that junk e-mail carried by its network dropped by some 75 percent this year. The daily average number of e-mails blocked by AOL's spam filters fell by 50 percent to about 1.2 million e-mails in late 2004 from a high of 2.4 billion in 2003, AOL said.

AOL attributes its success to improved technical anti-spam countermeasures by the company's anti-spam operations and postmaster teams, as well as stepped-up enforcement actions carried out by government authorities and by AOL under tougher federal and state anti-spam laws.

As for what computer users can do to thwart spam, Mastoras offers some common-sense advice: "Never open an e-mail that looks questionable, and don't reply to such messages, because that lets spammers know you have a working e-mail address," he said. Enterprises would be well advised to increase the security at their e-mail gateways, he added.

2004: Good and Bad for Security

Experts agree: 2004 was the best of times and the worst of times for those concerned about security. It was a year with high-profile arrests of virus authors, and the explosion of online crimes, from cyber-extortion to identity theft, a year in which ISPs won millions in damages from spammers, and spam messages increased by 40 percent.

In hindsight, 2004 may be looked back upon as the year that a long tradition of hobbyist hackers and flashy, but harmless, viruses gave way to shadowy, professional online crime syndicates. The professionals were armed with virulent new threats designed to separate Internet users from their cash, according to interviews with leading security experts.

With that in mind, here's a look at some of the most important technology security stories and trends of the last year:

Online identity theft through phishing scams was the run-away security story of 2004, due to the explosive growth in such attacks.

Phishing scams are online crimes that use spam to direct Internet users to Web sites controlled by thieves, but designed to look like legitimate e-commerce sites. Users are asked to provide sensitive information, often under the guise of updating account information, which is then captured by the thieves.

E-mail security vendor MessageLabs blocked an insignificant trickle of 279 such scams in September 2003. By September 2004, that trickle swelled to a flood of more than 2 million messages, according to a statement from the company. In all, MessageLabs says it blocked 18 million phishing e-mail messages in 2004.

The Anti-Phishing Working Group watched the number of reported phishing Web sites increase by an average of 28 percent each month between July and November. The average phishing Web site operated for six days before being shut down, according to Peter Cassidy, secretary general of the group.

"Phishing has really exploded, it's been one of the biggest problems we've had," says Mikko Hyppnen of Finnish antivirus company F-Secure.

Not since the days of Ancient Greece have Trojans been as much a part of popular conversation as they were in 2004, when an explosion in Trojan horse programs turned countless Internet-connected computers into tools for malicious hackers and international online crime organizations.

Carried on the back of e-mail and Internet worms, an eye-popping parade of back door Trojans marched onto vulnerable computers since January.

One typical example is the ubiquitous RBot, a Trojan program that spreads using a number of methods. The program can collect system information, download and execute files, launch a denial-of-service (DOS) attack, and even remotely control a connected Web cam.

RBOT-A, the first version of the worm-like Trojan, was identified in March 2004. The latest, RBot RN was identified on December 13, according to U.K. antivirus company Sophos. In just nine months, there were 480 different versions of the Trojan.

Trojan horse and backdoor programs are not new, but the rapid growth in their use in 2004 was a product of cooperation between virus writers, online criminals and spammers, says Jesse Villa, technical product manager at Frontbridge Technologies.

Trojans have been silent actors in a number of high-profile crimes, including the theft in 2003 of source code for the "Half-Life 2" video game. A Trojan horse program named Banker-AJ infected computers and waited until users visited online banking sites, at which point the program logged user keystrokes and captured account information, says Gregg Mastoras, senior security analyst at Sophos.

More Trojans have also led to an increase in the number of "botnets," distributed networks of compromised machines that act as "zombies" in spam campaigns or DDOS (distributed DOS) attacks.

"At the end of last year we knew of about 2000 botnets. Towards the end of this year, we're looking at about 300,000," Villa says.

Those networks range from 100 infected PCs to networks of thousands of zombie computers, which are rented out to aspiring spammers or for targeted DOS attacks used in online extortion rackets, Villa says.

"Bots have largely gone ignored," says Hyppnen. "You don't see alerts on bots, however they have probably been a bigger problem [than viruses]."

But the news wasn't all bad. While online crimes skyrocketed in 2004, there were also a number of high-profile arrests of those involved in cybercrimes.

In May, German authorities arrested 18-year-old Sven Jaschan, who admitted to creating and releasing the Netsky and Sasser Internet worms, and a 21-year-old German man who admitted to creating the Agobot and Phatbot Trojans.

There were other victories as well, including the June arrest of those believed to be behind the 2003 "Half-Life 2" source code theft and a September arrest of a man believed to be connected to the theft of source code belonging to Cisco Systems. In October, the U.S. Department of Justice arrested 19 people in connection to an online "carding" ring that traded information about stolen identity and credit card information online.

In 2005, some combination of tougher law enforcement and tighter security is the best way to stem the tide of malicious and criminal behavior online, experts agree.

To stop identity theft, banks, e-commerce companies and consumers need to look hard at strong user authentication technology, says Sophos' Mastoras.

"In the [European Union, banks are already moving away from static passwords. I think that will be a trend that will happen in the U.S. as well," he says.

E-mail sender authentication technologies such as Domain Keys from Yahoo and Sender ID from Microsoft need to be broadly adopted - a move that would make life tougher for those behind phishing scams, which often use forged e-mail sender addresses to trick unsuspecting e-mail recipients, says Mastoras.

ISPs also have to begin sharing what they know about Internet attacks and compromised computers on their networks, Villa says.

"This is a long term problem and we have to work together to combat it," he says.

Phishing, Spyware, Others Plague Internet

Computer worms raced around the world, leaving behind tools that spread spam. Scammers sent e-mail to trick bank account holders into revealing passwords. Rogue programs known as "spyware" hijacked Web browsers and crippled computers.

These were among the top Internet threats of 2004 as the perpetrators grew smarter and more sophisticated, driven more than ever by economic gains. And while technology to combat such threats has improved, experts concede that's not enough to address what's bound to emerge in the coming year.

"The bottom line is, there is no silver bullet technology," said Gregg Mastoras, senior security analyst at security vendor Sophos Inc. "I just

don't think users are educated enough when they are on machines and what they are doing with it."

The past year saw more industry attention to security: Microsoft Corp. upgraded its flagship Windows XP operating system, closing many loopholes and turning on a built-in firewall to thwart attacks. America Online Inc. gave away free security tools, and computer makers began installing software to combat spyware.

Dozens of products and services were developed to attack "phishing" - e-mail pretending to be from trusted names such as Citibank or Paypal, but directing recipients to rogue sites.

But developers of malicious code have gotten better at automating their tools, as well as sharing information about vulnerabilities and techniques to exploit them through underground message boards and chat rooms, said Mark Rasch, chief security counsel for Solutionary Inc.

No longer are bragging rights the primary motive.

"It used to be cool to bring down sites, almost (like) graffiti for the 21st century," said Arthur Coviello Jr., chief executive for RSA Security Inc. "Today's worms and viruses are far more detailed, and specific attacks are directed at individuals and businesses for the purpose of economic, ill-gotten gains."

Virus writers have found new ways to infiltrate computers and networks, bypassing the protections inspired by their earlier methods of attack.

For instance, with more network administrators blocking attachments to stop viruses from spreading via e-mail, hackers managed in June to covert popular Web sites into virus transmitters by taking advantage of known flaws with Microsoft products.

They've also used viruses like "Mydoom" to deposit programs that let them take over infected PCs - and then use them to relay spam or launch attacks on Web sites like Microsoft's. Ninety percent of viruses in 2004 carried a "backdoor" mechanism, compared with less than half in 2003, said Alfred Huger of Symantec Corp.

And once they've commandeered such PCs, they form networks of "zombies." Spammers buy access to these networks so they can send e-mail that appears to come from legitimate home computers, making them harder to tag as junk.

"They are well organized on the black market," said John Levine, co-author of "The Internet for Dummies."

Much of the malicious code appears to originate in countries without adequate laws to prosecute, experts say.

Meanwhile, law enforcement agencies and service providers are only beginning to establish guidelines for jointly chasing suspects who can move about with stealth in a medium that knows no borders.

Security experts rank phishing and spyware as the greatest threats for 2005, given how clever their developers have gotten in the past year.

Unlike spam pitching relatively cheap products like Vioxx, phishing scams can quickly drain entire bank accounts of unsuspecting users.

The number of rogue sites used for such scams grew sevenfold in just four months - to 1,518 in November, from 221 in July - according to Websense Inc., which compiles such data for the industry-backed Anti-Phishing Working Group.

By fall, phishers began automating their scams, embedding scripts within e-mail to launch a legitimate site like Citibank's along with a fake pop-up window that captures account information. Many users would mistakenly believe the pop-up came from the bank, said Jim Murphy, director of product marketing at SurfControl plc.

Spyware infections, once limited to careless downloads of free software, proliferated in 2004 as security gaps in Microsoft's Windows operating systems and Internet Explorer browser were exposed and exploited. These holes were used to slip in programs which can change a browser's home page or pop up endless ads.

Some security experts recommend using a non-Microsoft browser like Mozilla Firefox to reduce spyware and other threats. But in 2005, flaws with those alternatives are likely to emerge as they become more popular and more heavily scrutinized.

The coming year could also mean more threats via cell phones, instant messaging software and Internet-based phone systems, as well as desktop search utilities being developed by Microsoft, Google Inc. and others.

Users will need to bear the responsibility for security as much as software developers and service providers, said Johannes Ullrich, chief technology officer with the SANS Internet Storm Center, a research organization.

"Think about traffic," he said. "You do need good cars. You need good drivers. You need good roads. If any one of those isn't there, you'll end up with accidents."

China Launches Next-Generation Internet

China is rolling out the first network based on Internet Protocol Version 6 (IPv6) technology, a major component of the next-generation Internet.

Dubbed CERNET2 (China Education and Research Network), the new backbone network connects 25 universities in 20 cities.

Officials claim top transmission speeds of 2.5 to 10 gigabits per second, with a trial connecting schools in Beijing and Tianjin reaching 40 gigabits per second. Coverage is expected to expand to 100 universities in the near future.

A key advantage of IPv6 is that it can address the shortage of IP addresses.

Under current Internet systems based on IPv4 technology, Chinese officials said, the U.S. controls 74 percent of some 4 billion IP addresses, while the number of addresses that China has is about equal to a single campus of the University of California, despite the fact that China has 80 million Internet users.

As a result, Asian countries, including China, Japan and South Korea, are

focused on IPv6 technology.

The National Development Reform Commission (NDRC) set up a China Next-Generation Internet (CNGI) fund of 1.4 billion yuan (US\$169 million) to support six next-generation Internet networks. Half of the funds are earmarked for CERNET2-related projects, while the remainder goes to five telecom operators.

Much of the key CERNET2 equipment, including routers, is provided by Chinese telecom equipment giant Huawei Technologies and Tsinghua Bit-Way.

"We were a learner and follower in the development of the first-generation Internet, but we have caught up with world's leaders in the next-generation Internet ... and won respect and attention from the international community," says Wu Jianping, director of the CERNET expert committee, in a statement.

Interest in IPv6 is growing, with the Internet Corporation for Assigned Names and Numbers (ICANN), which officially introduced the technology in July, claiming it will provide trillions more addresses than the IPv4 system used by most networks today.

The U.S. Department of Commerce handed ICANN the task of coordinating the Internet's naming and numbering system globally, as rapid growth in the use of the Web had raised fears about a potential scarcity of IP addresses.

Networking giant Cisco recently announced it will invest \$12 million in an R&D center that focuses on the development of IP-based networking technologies, including IPv6.

=~::~~==

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.